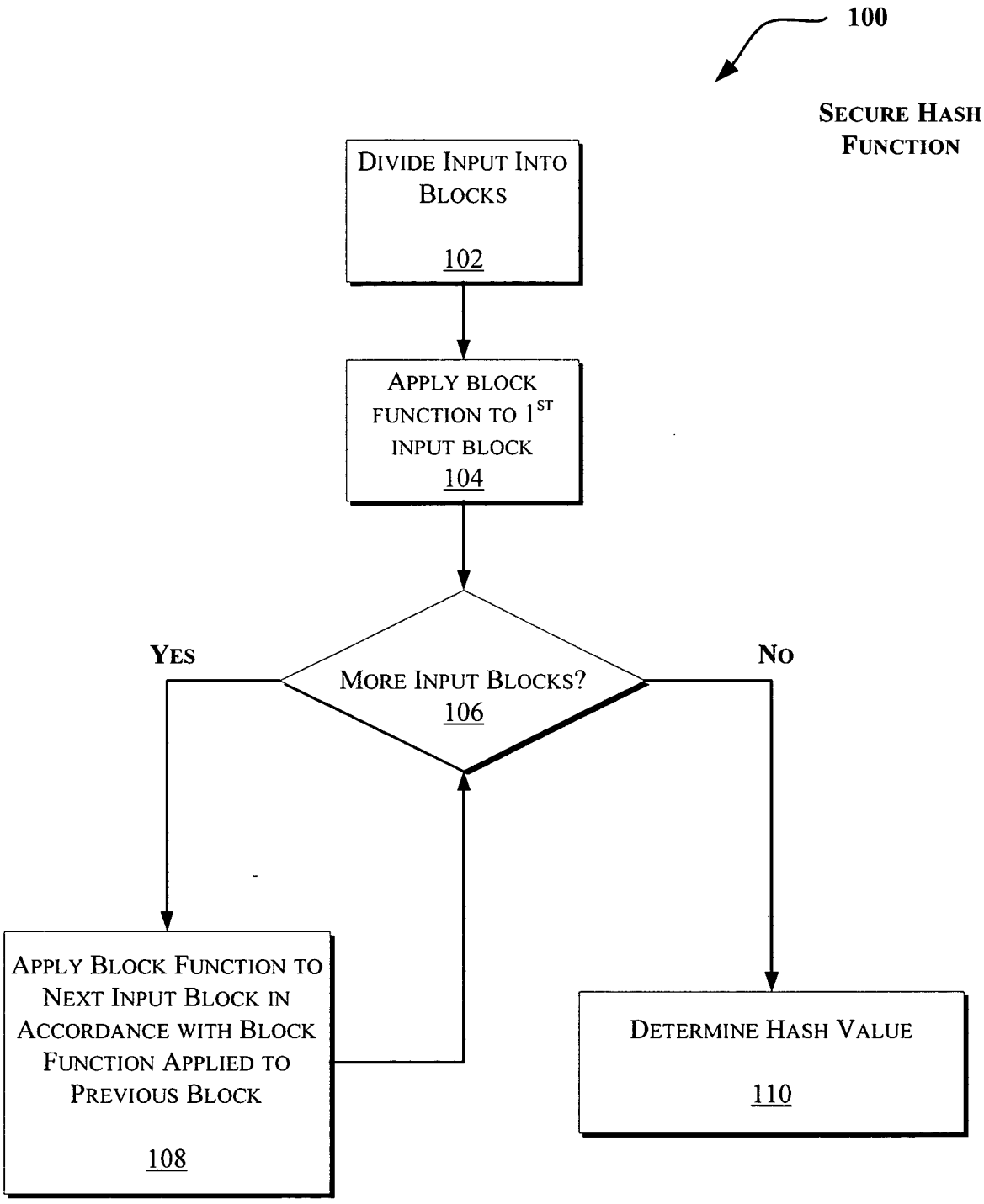
100
SECURE HASH FUNCTION
DIVIDE INPUT INTO BLOCKS
102
APPLY BLOCK FUNCTION TO 1ST INPUT BLOCK
104
MORE INPUT BLOCKS?
106
YES
NO
APPLY BLOCK FUNCTION TO NEXT INPUT BLOCK IN ACCORDANCE WITH BLOCK FUNCTION APPLIED TO PREVIOUS BLOCK
108
DETERMINE HASH VALUE
110

FIG. 1

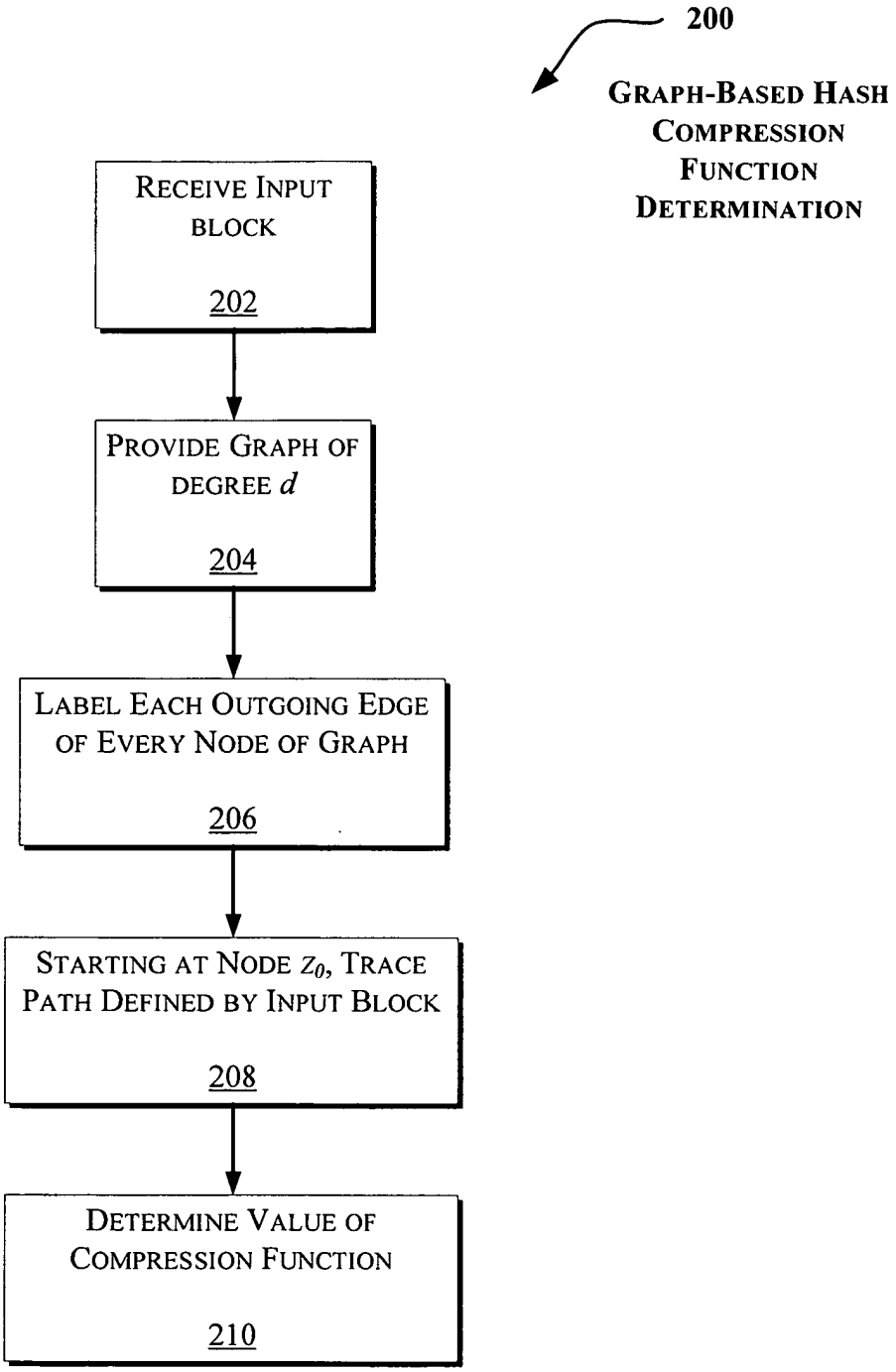
200
GRAPH-BASED HASH COMPRESSION FUNCTION DETERMINATION
RECEIVE INPUT BLOCK
202
PROVIDE GRAPH OF DEGREE d
204
LABEL EACH OUTGOING EDGE OF EVERY NODE OF GRAPH
206
STARTING AT NODE z_0, TRACE PATH DEFINED BY INPUT BLOCK
208
DETERMINE VALUE OF COMPRESSION FUNCTION
210

FIG. 2

$$\sigma_1 = \begin{pmatrix} 3 & 1 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \sigma_7 = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \sigma_8 = \begin{pmatrix} 3 & 2 & 2 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

FIG. 3

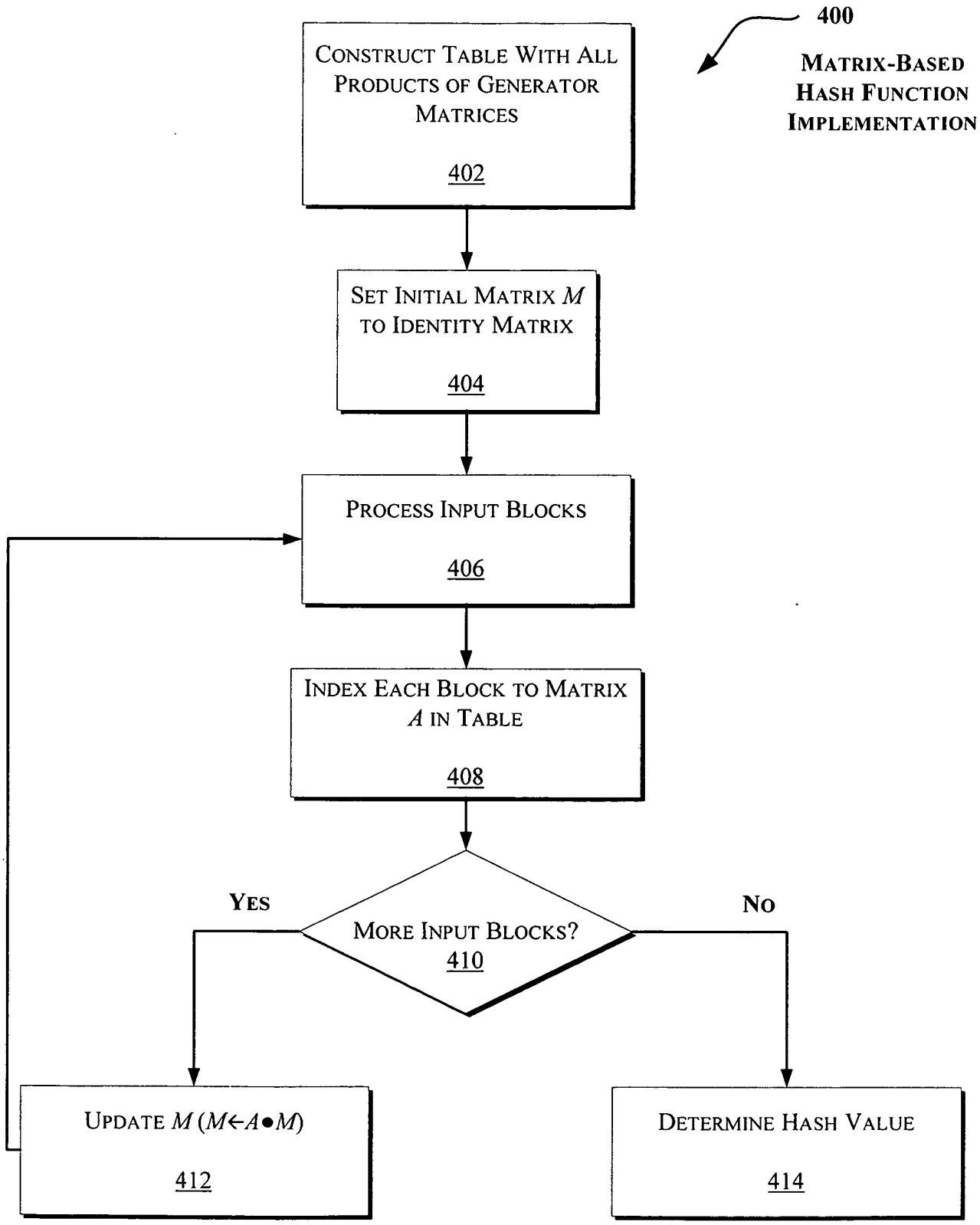
400
MATRIX-BASED HASH FUNCTION IMPLEMENTATION
CONSTRUCT TABLE WITH ALL PRODUCTS OF GENERATOR MATRICES
402
SET INITIAL MATRIX M TO IDENTITY MATRIX
404
PROCESS INPUT BLOCKS
406
INDEX EACH BLOCK TO MATRIX A IN TABLE
408
MORE INPUT BLOCKS?
410
YES
NO
UPDATE M (M←A•M)
412
DETERMINE HASH VALUE
414

FIG. 4

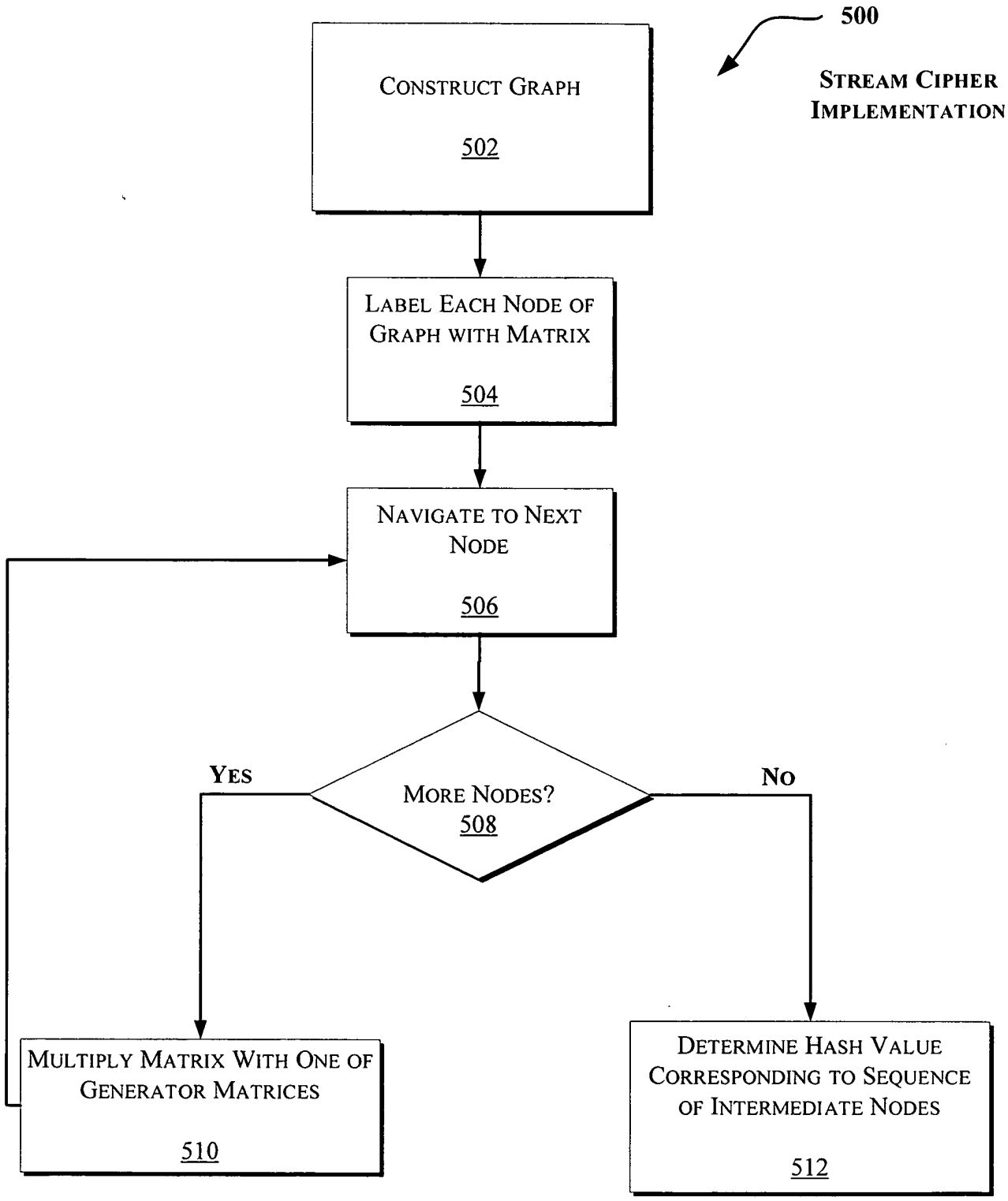
500
STREAM CIPHER IMPLEMENTATION
CONSTRUCT GRAPH
502
LABEL EACH NODE OF GRAPH WITH MATRIX
504
NAVIGATE TO NEXT NODE
506
MORE NODES?
508
YES
NO
MULTIPLY MATRIX WITH ONE OF GENERATOR MATRICES
510
DETERMINE HASH VALUE CORRESPONDING TO SEQUENCE OF INTERMEDIATE NODES
512

FIG. 5

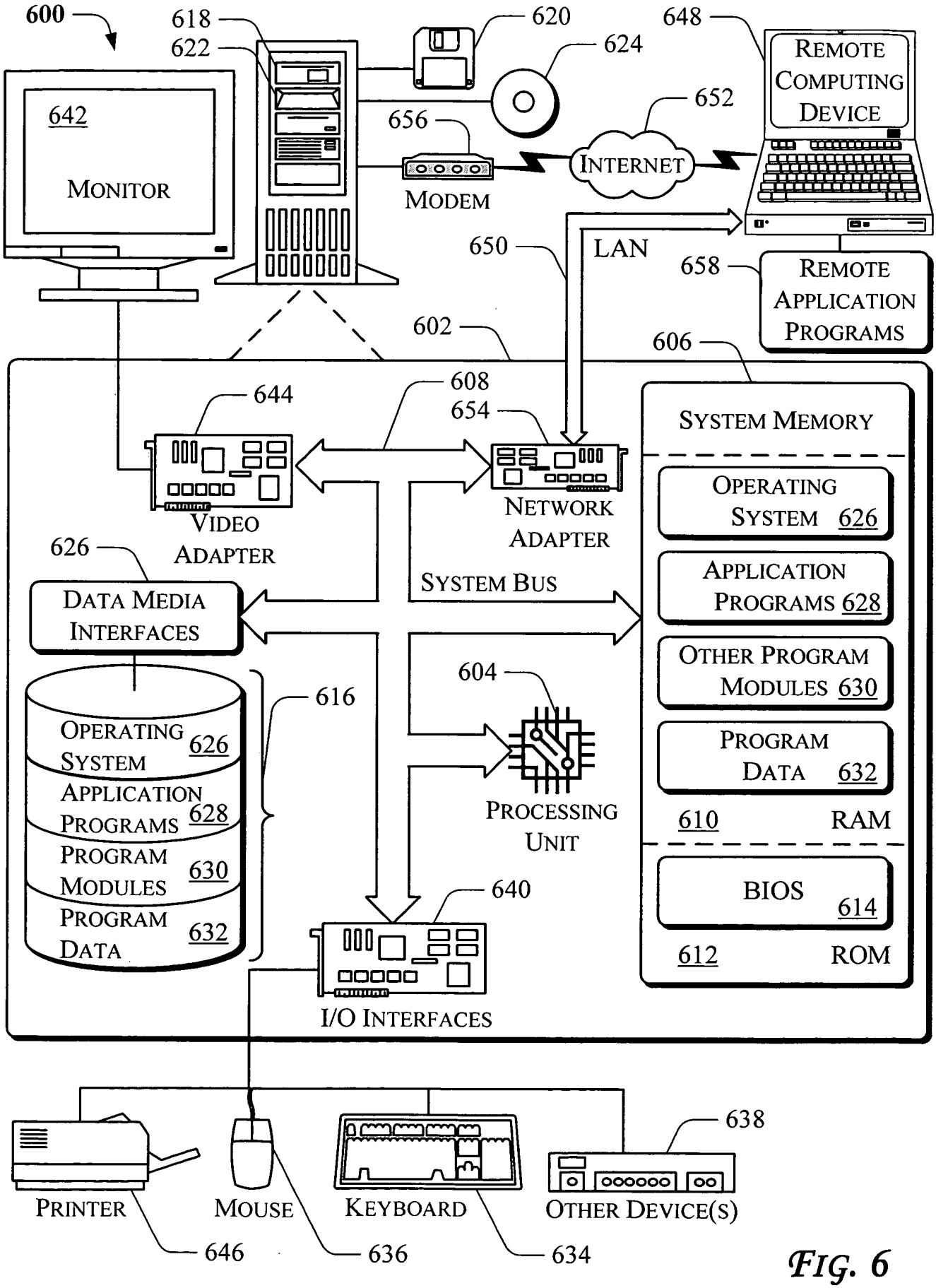
600
618
622
620
624
648
REMOTE COMPUTING DEVICE
642
MONITOR
656
MODEM
652
INTERNET
650
LAN
658
REMOTE APPLICATION PROGRAMS
602
606
644
608
654
SYSTEM MEMORY
VIDEO ADAPTER
NETWORK ADAPTER
OPERATING SYSTEM 626
626
DATA MEDIA INTERFACES
SYSTEM BUS
APPLICATION PROGRAMS 628
OTHER PROGRAM MODULES 630
604
616
OPERATING SYSTEM 626
APPLICATION PROGRAMS 628
PROGRAM MODULES 630
PROGRAM DATA 632
PROCESSING UNIT
PROGRAM DATA 632
610
RAM
BIOS 614
612
ROM
640
I/O INTERFACES
638
PRINTER
MOUSE
KEYBOARD
OTHER DEVICE(S)
646
636
634

FIG. 6